**УДК 343.98**

# НАЗНАЧЕНИЕ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПО МАТЕРИАЛАМ ПРОВЕРКИ И УГОЛОВНЫМ ДЕЛАМ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

**Д. И. Шнейдерова**
Могилевский институт МВД Республики Беларусь,
преподаватель кафедры уголовного процесса и криминалистики

***Аннотация.*** *В статье автором рассматриваются проблемные вопросы назначения компьютерно-технической экспертизы по делам о хищениях в сфере оборота криптовалют, вытекающие из специфики данной категории преступлений. Обращается внимание на сущность экспертизы, выделение ее типизации, объекты, определение предмета и формулировку вопросов, влияние выбора экспертного учреждения или эксперта на результаты исследования.*

***Ключевые слова:*** *криптовалюта, хищение, экспертиза, эксперт, специальные знания, реестр, компьютер, носитель информации.*

***Annotation.*** *The author of the article considers problematic questions of the appointment of computer expertise in cases of theft in the field of turnover of cryptocurrencies, arising from the specifics of this category of crimes. Attention is paid to the essence of expertise, the definition of its typology, objects, determination of the subject and formulation of questions, the impact of the choice of expert institution or an expert on the results of the investigation.*

***Keywords:*** *cryptocurrency, theft, expertise, expert, specialist knowledge, registry, computer, storage medium.*

Легализация оборота криптовалют в Республике Беларусь послужила отправной точкой в формировании нового блока преступлений, совершаемых с использованием информационных технологий, — хищений в сфере оборота криптовалют, процесс расследования которых не обходится без использования специальных знаний в области IT. Процессуальной формой использования таких знаний является проведение экспертиз, составляемые по итогам которых заключения признаются источниками доказательственной информации по уголовному делу согласно ч. 2 ст. 88 Уголовно-процессуального кодекса Республики Беларусь [1]. Специфика хищений в сфере оборота криптовалют влияет на разновидности экспертиз, назначаемых по данной категории дел. Так, в зависимости от объекта экспертного исследования, как правило, назначается компьютерно-техническая экспертиза (компьютеры, съемные носители данных, ноутбуки, программы) и/или экспертиза радиоэлектронных устройств и электробытовой техники (смартфоны, планшеты). В рамках настоящей статьи подлежат рассмотрению особенности и проблемные аспекты назначения компьютерно-технической экспертизы (далее — КТЭ).

КТЭ относится к группе технических экспертиз и может рассматриваться как исследование, проводимое лицом, обладающим специальными знаниями в области информационных технологий, по постановлению следователя (лица, производящего дознание), направленное на выявление, фиксацию, анализ компьютерной информации, исследование технических устройств и программ, используемых для ее создания, хранения, обработки, модификации и передачи, с целью дачи заключения по поставленным в постановлении вопросам. Круг вопросов, формулируемых эксперту при назначении КТЭ, образуется исходя из ее предмета, который, по мнению А. И. Шведа, нематериален и представляет собой информацию, имеющую характер вывода, т. е. то, что устанавливается экспертом при исследовании предоставленных материалов [2, с. 55]. Так, предметом КТЭ являются фактические данные об обстоятельствах разработки и эксплуатации компьютерных средств и систем, обеспечивающих реализацию информационных процессов [2, с. 155].

Исходя из изложенного, можно выделить основные объекты КТЭ: материальные — технические устройства (компьютеры, любые носители информации — винчестеры, флеш-карты, оптические диски и т. д., сетевые аппаратные средства) и цифровые — компьютерная информация, зафиксированная в памяти технических устройств (файлы любого формата, в т. ч. веб-страницы, каталоги, программы и приложения, их исходные коды, операционные системы и их образы, базы данных, протоколы работы системы и отдельных программ, алгоритмы). Поскольку криптовалюты являются разновидностью компьютерной информации, то в обеспечении их создания и функционирования задействованы по большей части все из указанных объектов. К примеру, среди материальных объектов, кроме компьютеров, можно отметить аппаратные криптокошельки, среди цифровых — базы данных на блокчейне, программы криптокошельков, криптобирж и обменников, мессенджеров и социальных сетей, электронной почты, браузеров, веб-страницы интернет-ресурсов (в т. ч. кошельков, бирж и обменников, если доступ осуществляется через браузер), лог-файлы программ и иные.

В теории отдельными авторами проводится типизация КТЭ в зависимости от объекта экспертного исследования. Так, Е. Р. Россинская выделяет аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную и компьютерно-сетевую экспертизы [3, с. 37], В. А. Мещеряков — аппаратно-техническую, программно-техническую, информационную и интегральную компьютерно-техническую экспертизы [4, с. 33]. Однако с точки зрения практической деятельности такое деление при назначении экспертизы не проводится, поскольку при любых обстоятельствах эксперту направляется техническое устройство (носитель данных), без которого цифровая информация

существовать не может, следовательно, первоначально исследованию подвергается устройство (его вид, общие характеристики), а только потом — цифровое содержимое его хранилища, даже если вопрос ставился только об обнаружении и извлечении некоторой информации или о функциональных возможностях программы.

Поскольку процессуальным основанием для проведения КТЭ является постановление о ее назначении, то грамотное его составление — ключевая задача следователя (лица, производящего дознание), так как от содержания данного процессуального документа во многом зависит результат предстоящего экспертного исследования. Такая зависимость вытекает из правильности постановки вопросов эксперту, исходя из характера предоставляемого на экспертизу материального объекта, подбора и приложения необходимых материалов из уголовного дела, способствующих установлению искомых фактических данных в процессе исследования, а также выбора экспертного учреждения или непосредственно эксперта, которому поручается проведение КТЭ. Определение указанных обстоятельств является не только первостепенной задачей на этапе назначения КТЭ, но и одновременно вызывает ряд проблемных вопросов, связанных со спецификой хищения. В первую очередь следователь сталкивается с необходимостью составления перечня вопросов, которые могут быть разрешены экспертом в рамках исследования. Вопросы предопределяют цель назначения экспертизы, т. е. результат, который необходимо получить следователю (лицу, производящему дознание), чтобы проверить следственные версии, получить новые фактические обстоятельства, влияющие на возбуждение дела или доказывание вины подозреваемого.

Постановке вопросов предшествует исследование лицом, назначающим КТЭ, материального объекта, направляемого на экспертизу. Поскольку такими объектами в рамках КТЭ являются компьютеры, накопители данных и аппаратные криптокошельки, следователи (лица, производящие дознание) не производят первоначальный осмотр их цифрового содержимого в целях обеспечения сохранности данных, а сразу направляют указанные устройства эксперту для безопасного копирования информации, в т. ч. поиска и приведения в вид, пригодный для осмотра, удаленных, скрытых, зашифрованных, поврежденных файлов. По причине неосведомленности о содержимом памяти объекта постановка вопросов носит общий характер, а сами вопросы выбираются из разработанных справочниками перечней случайным образом как наиболее подходящие под сложившуюся следственную ситуацию и способ совершения хищения криптовалют. Исходя из этого, предмет КТЭ значительно увеличивается и, как следствие, на проведение экспертизы и анализ выявленной информации

затрачивается в несколько раз больше времени, чем если бы перед экспертом ставились конкретные, действительно требующие решения задачи.

Кроме того, назначение КТЭ во многих случаях сводится к извлечению цифровой информации из памяти носителя посредством использования программных и аппаратно-программных средств, которые также имеются на вооружении криминалистических отделов подразделений Следственного комитета Республики Беларусь и управлений по противодействию киберпреступности Министерства внутренних дел. В связи с этим представляется целесообразным привлекать сотрудников указанных подразделений к участию в проведении таких следственных действий, как осмотр места происшествия или осмотр предмета и компьютерной информации, в качестве специалистов, которые имеют навыки работы и техническую возможность осуществить те же действия по поиску и копированию информации с компьютерных устройств и носителей, что и эксперты в рамках КТЭ. В случаях, если на определенной территории такие подразделения отсутствуют, а прибытие соответствующего специалиста длительно по времени и может угрожать потерей информации, следователю (лицу, производящему дознание) либо эксперту-криминалисту, привлеченному к осмотру в составе следственно-оперативной группы, целесообразно получить образ системы или жесткого диска посредством использования загрузочной флеш-карты с предустановленной на ней программой специального назначения (например, Macrium, Acronis, Paragom Backup and Recovery, Handy Backup, Drive Image XML и иные), но только при условии, что на устройствах не запущены рабочие процессы неизвестных программ. Работе с такими программными продуктами следует обучать сотрудников правоохранительных органов в рамках проведения тематических курсов повышения квалификации. Видится, что предложенные меры позволят значительно сократить сроки на получение имеющей значение для расследования хищений информации, конкретизировать предмет КТЭ, снизить нагрузку экспертов и предоставить им больше времени на решение более сложных задач, чем копирование данных.

В случаях, если полученная информация находится в зашифрованном виде или при помощи подручных программ не удалось восстановить удаленные файлы или получить доступ к зашифрованным и скрытым каталогам и файлам, либо неизвестны функциональные возможности отдельных программ, либо не представилось возможным создание образа системы или жесткого диска по месту нахождения устройства, то следует прибегнуть к КТЭ. При этом, кроме отсутствия выборки узконаправленных вопросов, имеют место проблемы, связанные с незнанием или неправильным применением терминологии. Такие проблемы приводят к тому, что эксперт не может дать ответ на поставленный вопрос ввиду его некорректности и изменить формулировку вопроса

самостоятельно также не может, так как не наделен соответствующей компетенцией. Изменение вопросов возможно только посредством вынесения лицом, назначившим экспертизу, нового постановления с отзывом без исполнения первоначального, что затягивает процесс получения доказательственной информации и, соответственно, процесс расследования [2, с. 56]. В этой связи по делам о хищениях в сфере оборота криптовалют видится целесообразным ввиду специфики предмета преступного посягательства и используемых в механизме хищения технических и программных средств перед назначением КТЭ обязательное предварительное консультирование со специалистом, которому будет поручено ее проведение, для правильной постановки вопросов и тем самым избежания повторного вынесения постановления по одним и тем же объектам. По результатам анкетирования следователей подразделений Следственного комитета Республики Беларусь, специализирующихся на расследовании киберпреступлений, 56 % респондентов находят предложенную меру необходимой во всех случаях назначения КТЭ, 39 % — только в случаях, если не обладают достаточными знаниями об объекте экспертизы. Приведенные показатели свидетельствуют об актуальности и практической значимости предложенной меры.

Немаловажным является и выбор экспертного учреждения или непосредственного эксперта, которому можно поручить проведение КТЭ по хищениям в сфере оборота криптовалют. В Республике Беларусь ведется Реестр судебно-экспертных организаций и индивидуальных предпринимателей, осуществляющих деятельность по проведению экспертиз на основании лицензии, анализ которого позволил определить, что КТЭ проводится как государственными экспертными учреждениями (в Центральном аппарате, областных управлениях и г. Минска Государственного комитета судебных экспертиз Республики Беларусь, а также в семи его межрайонных отделах: Барановичском, Новополоцком, Оршанском, Мозырском, Лидском, Борисовском, Бобруйском), так и негосударственным — ООО «ПравитЭксперт». На основании сведений реестра лицо, назначающее КТЭ, может не только достоверно определить организацию, которой осуществляется КТЭ, но и посредством взаимосвязи с ней реализовать выбор эксперта, квалификация и опыт работы которого позволят провести требуемое исследование.

Таким образом, при назначении КТЭ по делам о хищениях в сфере оборота криптовалют следователю (лицу, производящему дознание) необходимо в первую очередь определить объекты, которые могут быть подвергнуты экспертному исследованию, выбрать экспертное учреждение, на базе которого имеются специалисты, квалифицированные на проведение КТЭ по направляемым объектам, после чего предварительно проконсультироваться с экспертом, которому непосредственно будет поручена назначаемая КТЭ, с целью

грамотной формулировки вопросов, установления возможности проведения экспертизы в целом, а также выяснения сроков ее производства.

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 20.07.2022 г. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

2. Швед А. И. Судебная экспертиза. Минск : Форум, 2022. 296 с. Вернуться к статье

3. Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестн. Ун-та им. О. Е. Кутафина (МГЮА). 2019. № 5. С. 31–44. Вернуться к статье

4. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. … д-ра юрид. наук : 12.00.09 / Воронеж. гос. ун-т. Воронеж, 2001. 40 с. Вернуться к статье